UNITED STATES PATENT AND TRADEMARK OFFICE

A

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/066,252	01/31/2002	Massimiliano Antonio Poletto	12221-012001	2792

26161 7590 09/02/2005

FISH & RICHARDSON PC
P.O. BOX 1022
MINNEAPOLIS, MN 55440-1022

EXAMINER	
NALVEN, ANDREW L	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 09/02/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/066,252	POLETTO ET AL.	
	Examiner	Art Unit	
	Andrew L. Nalven	2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *31 January 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-25 and 27-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-25 and 27-34* is/are rejected.

7)☒ Claim(s) *11 and 18* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *31 January 2002* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Claims 1-25 and 27-34 are pending.

Examiner notes that the original presentation of the claims provided no claim 26.

Claim Objections

1. Claims 11 and 18 are objected to because of the following informalities: Claim 11 contains the typo "monitor" on line 5. Examiner has interpreted the intended recitation to be "monitor." Claim 18 contains the typo "for one for the" on line 32. Appropriate correction is required.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claims 1, 7, 11,12-14, 14-17, 22, 24, and 29 rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

3. With regards to claim 1, 7, 11, 24, and 29, the cited claims define a device that examines traffic "as if the device was disposed on links that are downstream from links that the provisioned monitor is disposed on." Examiner in unclear as to what property

this limitation instills upon the device. Further, Examiner can ascertain no structural elements either explicitly or implicitly from this limitation.

4. With regards to claims 12-14, 16, 17, the cited claims recite the limitations "the gateways" and "the gateway." There is insufficient antecedent basis for the limitations in these claims.

5. With regards to claims 14-16, the cited claims recite the limitation "global packet log." There is insufficient antecedent basis for these limitations in the claims.

6. With regards to claim 22, the cited claim recites the limitation "the hosting provider." There is insufficient antecedent basis for this limitation.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

7. Claims 1-34 are rejected under 35 U.S.C. 102(e) as being anticipated by Porras et al US Patent No. 6,321,338.

8. With regards to claim 1, Porras teaches a device that collects statistical information on packets that are sent between a network and the data center for a

plurality of customers by examining traffic as if the device was disposed on links that are downstream from the links that the provisioned monitor is on (Porras, column 3 lines 31-42, Figure 1).

9. With regards to claims 2 and 7, Porras teaches the monitoring device coupled to the control center through a dedicated private network (Porras, column 10 lines 27-62).

10. With regards to claim 3, Porras teaches a communication process that communicates statistics with the control center and which receives queries or instructions from the control center (Porras, column 4 lines 19-47, column 8 lines 47-65).

11. With regards to claims 4, 8, 21, 28, 29-30, and 34 Porras teaches a process to install filters to thwart denial of service attacks by removing network traffic that is deemed part of an attack (Porras, column 12 lines 7-18).

12. With regards to claims 5, 9, 27, Porras teaches the monitoring device being a data collector device (Porras, column 4 lines 61-67, event record).

13. With regards to claim 6, Porras teaches a process to aggregate traffic from the various links and to produce logs and detection heuristics (Porras, column 5 lines 4-36).

14. With regards to claim 10, Porras teaches the collecting occurring for inbound and outbound traffic (Porras, column 4 line 61 – column 5 line 6, transmitted and received).

15. With regards to claims 11, 13-14, 16, 24, Porras teaches a provisioned monitor that collects statistical information for a plurality of provisioned customers which are on links that are downstream from links that the provisioned monitor is on (Porras, column 3 line 66 – column 4 line 18, domain monitors subscribe to monitors), the provisioned

monitor maintaining separate counter logs for each provisioned customer (Porras, column 4 lines 61-67, event record) and a global counter log that accounts for all traffic seen on the link that the provisioned monitor is coupled to (Porras, column 5 lines 30-36).

16. With regards to claim 12, Porras teaches the gateways maintaining separate packet logs for each virtual monitor (Porras, column 7 lines 35-42).

17. With regards to claim 15, Porras teaches packet analysis for a particular virtual monitor happens by classifying packets based on addresses at the time of analysis (Porras, column 5 lines 4-30).

18. With regards to claim 17, Porras teaches the gateway being a clustered gateway and includes a plurality of probes and a cluster head, with the cluster head having a process to aggregate traffic from the probes and to produce separate counter logs for each provisioned customer and a global counter log, and produce detection heuristics (Porras, column 4 lines 19-47).

19. With regards to claim 18, Porras teaches the provisioned monitor including a virtual monitor for the physical link on which the provisioned monitor is deployed is configured to be an independent node in the network capable of issuing attack warnings and responses to attack queries independently from the virtual monitors of the provisioned monitor (Porras, column 8 lines 30-65).

20. With regards to claim 19, Porras teaches the provisioned monitor including all of the provisioned monitor's virtual monitors act as one node in the network (Porras, column 4 lines 48-62, Figure 1).

21. With regards to claim 20, Porras teaches the provisioned monitor acts as an intermediary between virtual monitors and the rest of the network and includes a process to maintain communications with the control center and to reply to attack queries (Porras, column 4 lines 19-47).

22. With regards to claim 22, Porras teaches a virtual monitor detecting an attack on a provisioned customer; information is conveyed both to the control center and to the hosting provider's management interface (Porras, column 3 line 67 – column 4 line 47).

23. With regards to claim 23, Porras teaches the control center being adapted to distinguish an attack on a single provisioned customer and an attack on the links to which the monitor is deployed (Porras, column 4 lines 31-36).

24. With regards to claim 25, Porras teaches the collection occurring at a gateway that passes network packets at the edge of the network (Porras, Figure 1).

25. With regards to claims 31-33, Porras teaches the communicating with a control center occurring on a downstream link basis over a dedicated hardened network (Porras, column 10 lines 27-39) to a control center that determines a response to the attack (Porras, column 4 lines 30-47).

Conclusion

26. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

27. Yavatkar et al US Patent No. 6,735,703 discloses a method for diagnosing network intrusion.

28. Ando et al US Patent No. 6,895,432 discloses an IP network system having an unauthorized intrusion detection function.

29. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Andrew L. Nalven whose telephone number is 571 272 3839. The examiner can normally be reached on Monday - Thursday 8-6, Alternate Fridays.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on 571 272 3838. The fax phone number for the organization where this application or proceeding is assigned is 571 273 8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Andrew Nalven

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100